Notic of Allowability	Application No. 10/092,544	Applicant(s) UEDA ET AL.	
	Examin r Ronald Baum	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *6/8/2006*.

2. ☒ The allowed claim(s) is/are *3,4,8,9 and 13-16*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

NASSER MOAZZAMI
PRIMARY EXAMINER

8/9/06

DETAILED ACTION

Examiner's Statement of Reasons for Allowance

1. Claims 3,4,8,9,13-16 are allowed over prior art.

2. This action is in reply to applicant's correspondence of 08 June 2006.

3. The following is an examiner's statement of reasons for the indication of allowable claimed subject matter.

4. As per claims 4,9,14-16 generally, prior art of record, Dömstedt, U.S. Patent 6,845,159 B1, fails to teach alone, or in combination, other than via hindsight, at the time of the invention, the features as discussed and remarked upon in the response of 6/8/2006 to office action of 3/9/2006.

Specifically, (as per claim 4, for example) prior art dealing with multiple/recursive cryptography generally, and more specifically, block chaining, multiple key symmetric encryption/decryption sequences, stream data oriented cryptography per se, is generally known to exist, (i.e., Wohlmacher,P.,'Introduction to the Taxonomy of Multiple Cryptography', Multimedia andSecurity Workshop, ACM '99, 10/1999, pp 7-15, wwwiti.cs.uni-magdeburg.de/iti_amsl/acm/acm99/GMD_report.pdf). Nowhere in the prior art is found collectively the *italicized* claim elements (i.e., the combination of steps whereas the key information as a function of a seed value as created/used for the cryptographic encryption/decryption functionality, is itself a function of the data block(s) position relative to previous block(s) in a hierarchy oriented data block chain; and the erasure of the key subsequent to the use in encryption.), at the time of the invention; serving to patently distinguish the invention from said prior art;

"4. An encryption method for encrypting information including

a plurality of continuous unit blocks having a reproduction order,

said plurality of unit blocks being encrypted

one unit block at a time,

wherein a *seed of an encryption key for encrypting a unit block is based*

on one or more unit blocks that are, in the reproduction order,

***before** the unit block* or

on information generated by encrypting one or more unit blocks

***before** the unit block*,

wherein the ***seed** of the encryption key is **chained** at least **twice***,

wherein an initial value IV of a seed of an encryption key used for

encrypting a first unit block of the plurality of unit blocks

having the reproduction order is stored,

wherein the *chain has a plurality of hierarchy levels*,

a first hierarchy level is encrypted based on

the initial value IV of the seed of the encryption key, and

a second and higher hierarchy levels are encrypted based on

*a **seed** of an encryption key at a **lower hierarchy level***,

wherein, *when encrypted unit blocks from*

the first unit block to

any given unit block of the encrypted information are decrypted for reproduction,

the initial value IV of the seed of

the encryption key that was stored is used, and

wherein, *when the reproduction of the unit blocks to the given unit block ends,*

the ***initial value IV of the seed of***

the encryption key that was stored ***is***

erased and

both

a ***seed*** *of an encryption key used for encrypting a unit block*

follows the given unit block *in the reproduction order and*

a ***seed*** *of an encryption key used for encrypting a unit block*

at another hierarchy level after *the given unit block are*

stored."

5. Dependent claims 3,8 and 13 are allowable by virtue of their dependencies.

Conclusion

6. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at (571) 272-4195. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

NASSER MOAZZAMI
PRIMARY EXAMINER

8/9/06